

Conjugacy in Artin Groups and Application to the Classification of Surfaces

Godelle Eddy, Kaplan Shmuel^{*†} and Teicher Mina

Abstract

We show that the double reversing algorithm proposed by Dehornoy in [3] for solving the word problem in the braid group can also be used to recognize the conjugates of powers of the generators in an Artin group of spherical type. The proof uses a characterization of these powers in terms of their fractional decomposition. This algorithm could have potential applications to braid-based cryptography; it also provides a fast method for testing a necessary condition in the classification of surfaces in algebraic geometry.

Keyword :conjugacy problem in Artin groups, surfaces classification.

MSC2000: 20F36, 14J10

1 Introduction and motivation

Let S be a finite set and let $M = (m_{s,t})_{s,t \in S}$ be a Coxeter matrix, that is, a symmetric matrix for which $m_{s,s} = 1$ for s in S and $m_{s,t} \in \mathbb{N} \cup \{\infty\} \setminus \{0, 1\}$ where $s \neq t$. The *Artin-Tits system associated to M* is the pair (A, S) where A is the group with presentation:

$$A = \left\langle S \mid \underbrace{s \ t \ s \ \cdots}_{m_{s,t} \text{ letters}} = \underbrace{t \ s \ t \ \cdots}_{m_{s,t} \text{ letters}} \text{ for } s, t \text{ in } S \text{ with } s \neq t \text{ and } m_{s,t} \neq \infty \right\rangle \quad (1)$$

A is called the *Artin group associated to M* . For instance, if $S = \{s_1, \dots, s_n\}$ with $m_{s_i, s_j} = 3$ for $|i - j| = 1$ and $m_{s_i, s_j} = 2$ otherwise, then the associated Artin group is the braid group on $n+1$ strings, B_{n+1} . If we add the relations $s^2 = 1$ for every s in S to the presentation of A , we get the Coxeter group W_S associated with A . When W_S is finite, we say that A is of *spherical type*. For instance, the braid group is of spherical type. The *Artin monoid A^+ associated to M* is the sub-monoid of A generated by S . This monoid has the same presentation as A but as monoid (see [14]). When A is of spherical type, any element β of A can be written in a unique way as an irreducible fraction $\beta = ab^{-1}$ with a and b in A^+ (see next section for precise definition). This fraction is called the *orthogonal splitting of β* .

The main result of this paper is the following:

^{*}Partially supported by the Emmy Noether Research Institute for Mathematics, Bar-Ilan University and the Minerva Foundation, Germany, and by the Excellency Center "Group theoretic methods in the study of algebraic varieties" of the National Science Foundation of Israel.

[†]The paper is part of the author's PhD. Thesis

Theorem 1.1 *Let (A, S) be an Artin-Tits system where A is of spherical type. If β is in A and is conjugated to a power of some element of S , then the orthogonal splitting of β is $\beta = bs^j b^{-1}$ with b in A^+ , s in S and j in \mathbb{Z} .*

We will derive from this theorem a quadratic (on the length of β) algorithm which detects these conjugated elements and returns b , s and j as above. Finding a fast algorithm which recognizes the conjugates of powers of the generators is useful both from a theoretic point of view (see [10] for instance) and from a practical point of view since the crypto-systems which use the braid group are based on the conjugacy problem. Also, following an idea suggested in [12] and in [13], it was proved in [11] that *braid monodromy factorization* can be used as a tool to classify surfaces up to diffeomorphism (see last section for more details). As an application of our current result, we deduce a second algorithm testing for a factorization to be a braid monodromy factorization of a cuspidal curve.

The paper is organized as follows: in Section 2 we prove Theorem 1.1, in Section 3, we explain the quadratic algorithm and compute its complexity. Finally, Section 4 is devoted to the application.

2 Proof of the Theorem 1.1

2.1 Preliminaries

In this part we recall some basic results on Artin groups which are needed in the proof of Theorem 1.1.

Let (A, S) be an Artin-Tits system where A is of spherical type, and let A^+ be the associated monoid of A . As both words in any relation of the presentation of A^+ have the same number of letters, we can define on A^+ a unique length function $\ell : A^+ \rightarrow \mathbb{N}$ which is a morphism of monoids and such that the length of an element of S is 1. We say that α *right-divides* β in A^+ if $\beta = \gamma\alpha$ for some γ in A^+ ; in that case, we write $\beta \succ \alpha$. We can define in the same way the left-divisibility and write $\alpha \prec \beta$ when α *left-divides* β in A^+ . Recall also that a monoid G^+ is said to be cancellative if any equality $\beta\alpha_1\gamma = \beta\alpha_2\gamma$ in G^+ implies $\alpha_1 = \alpha_2$.

Proposition 2.1 ([1]) *Let (A, S) be an Artin-Tits system where A is of spherical type and A^+ be the associated monoid of A .*

i) A^+ is cancellative.

ii) any two elements of A^+ have a right-l.c.m. $\alpha \vee_\succ \beta$ and a right-g.c.d. $\alpha \wedge_\succ \beta$ in A^+ for right-divisibility.

The same is true if we replace right by left.

iii) The right-gcd and the left-gcd of all elements in S are equal. We denoted by Δ_S this element.

iv) if $\alpha s = \beta t$ in A^+ with s and t in S distinct, then $m_{s,t} \neq \infty$ and there exists γ in A^+ such that $\alpha = \gamma \underbrace{\cdots t s t}_{m_{s,t}-1 \text{ letters}}$ and $\beta = \gamma \underbrace{\cdots s t s}_{m_{s,t}-1 \text{ letters}}$

v) Δ_S is quasi-central in A_S and Δ_S^2 is in the center in A_S ; in other words, there exists a permutation $\sigma : S \rightarrow S$ of order 1 or 2 such that $s\Delta_S = \Delta_S\sigma(s)$ for any s of S .

The key property of Artin groups of spherical type is the existence of the element Δ_S which allows to describe the group using the monoid:

Proposition 2.2 *Let (A, S) be an Artin-Tits system where A is of spherical type and let A^+ be the associated monoid of A .*

i) ([6] Paragraph 4) *Let β be in A ; then β can be written $\beta = \beta_1 \Delta_S^{-n}$ with β_1 in A^+ , and n in \mathbb{N} .*

ii) ([2] Theorem 2.6) *Let β be in A ; then there exists a unique pair (a, b) of elements of A^+ such that $a \wedge_\succ b = 1$ and $\beta = ab^{-1}$.*

We call the decomposition $\beta = ab^{-1}$ of ii) the (right) orthogonal splitting of β . In a similar way one can define the left orthogonal splitting $\beta = c^{-1}d$ of β .

Of course, since Δ_S is quasi-central, we can also in i) write $\beta = \Delta_S^{-n} \beta_2$ with β_2 in A^+ .

With this background, we are now ready to prove Theorem 1.1.

2.2 Proof of Theorem 1.1

We assume in the following that A_S is an Artin group of spherical type, and we choose β in A_S which is conjugated to a power of some element of S , that is $\beta = wt^jw^{-1}$ with w in A_S , t in S and j in \mathbb{Z} .

We will use the following easy result.

Lemma 2.3 *let t and u be distinct in S , let α be in A^+ and k in $\mathbb{N} - \{0\}$ such that u right-divides αt^k . Then $m_{t,u}$ is finite and $\underbrace{\cdots u t u}_{m_{t,u}-1 \text{ letters}}$ right-divides α .*

PROOF: This lemma is a direct consequence of Lemma 3.1 and Lemma 3.2 of [1] and is true in any, not necessarily spherical type Artin monoid. It can also be seen as a consequence of Proposition 2.1 i) and iv). \square

PROOF: (Theorem 1.1) If ab^{-1} is the orthogonal splitting of β then the orthogonal splitting of $\beta^{-1} = wt^{-j}w^{-1}$ is ba^{-1} . Hence it is enough to prove Theorem 1.1 when j is positive (the case $j = 0$ is obvious). So we assume j positive in the following.

By Proposition 2.2 i), there exists w_1 in A^+ such that $w = w_1 \Delta_S^{-k}$ with k in \mathbb{N} . Furthermore, Proposition 2.1 vi) states that Δ_S is quasi-central. Thus $\beta = wt^jw^{-1} = w_1 \Delta_S^{-k} t^j \Delta_S^k w_1^{-1} = w_1 (\sigma^k(t))^j w_1^{-1}$ with $\sigma^k(t)$ which is in S . Hence we can assume for the remaining of the proof that $w = w_1$ is in A^+ . Let us prove that the orthogonal splitting of β is bs^jb^{-1} for some b in A^+ and some s in S by induction on $\ell(w)$. If $wt^j \wedge_\succ w = 1$ then wt^jw^{-1} is the orthogonal splitting of β and we are done. This is, in particular, the case when $w = 1$; so assume $\ell(w) \geq 1$ and $wt^j \wedge_\succ w \neq 1$. Assume that the orthogonal splitting of $w's^jw'^{-1}$ for any w' in A^+ with $\ell(w') < \ell(w)$ and any s in S is of the required form. Since $wt^j \wedge_\succ w$ is different from 1, there exists u in S and w' in A^+ such that $w = w'u$ and $w't^j \succ u$. If $u = t$ then $\beta = w't^jw'^{-1}$ and we can apply the induction hypothesis since $\ell(w') = \ell(w) - 1$. Assume that u is different from t , then by Lemma 2.3 we have $w = w'' \underbrace{\cdots u t u}_{m_{t,u}-1 \text{ letters}}$ and $\beta = wt^jw^{-1} =$

$w'' \underbrace{\cdots u t u}_{m_{t,u}-1 \text{ letters}} t^j \underbrace{u^{-1} t^{-1} u^{-1} \cdots}_{m_{t,u}-1 \text{ letters}} w''^{-1} = w'' s^j w''^{-1}$ with s in $\{u, t\}$ such that $\underbrace{\cdots t u t}_{m_{t,u} \text{ letters}} =$
 $s \underbrace{\cdots u t u}_{m_{t,u}-1 \text{ letters}} .$ Since $\ell(w'') = \ell(w) - m_{t,u} + 1 < \ell(w)$, we can apply the induction hypothesis to

conclude. \square

Note that we can not expect to extend Theorem 1.1 to the family of Garside groups, which is a larger family than the one of Artin groups of spherical type (see [5]), since in $\langle a, b \mid aba = b^2 \rangle$ the normal form of ab^2a^{-1} is a^2b .

3 The algorithm

Before we describe our algorithm we note that an algorithm for solving the conjugacy problem in Garside groups was already given in [9]. Their solution, although not polynomial in general is polynomial in the case of the conjugacy class of powers of the group's generators. We present here a different approach, which is at least as efficient.

3.1 Description of the algorithm

We begin by recalling from [3] and [5] the details of the double reversing method proposed by Dehornoy to find the orthogonal splitting of β .

An Artin group of spherical type is a Garside group with Δ_S as it's Garside element([5]). In particular, M_S the set of all left divisors of Δ_S is closed under right-lcm and under left-lcm, and includes S ; the permutation σ of Proposition 2.1 v) can be extended to a permutation σ with order 2 of M_S such that for any x in M_S , one has $\sigma(x)\Delta_S = \Delta_S x$. Furthermore, there exists a (right) *complement* function $f : M_S \times M_S \rightarrow M_S$ such that $f(x, x)$ is the empty word for every x in M_S and $xf(y, x) = yf(x, y) = x \wedge_{\prec} y$ for any x, y in M_S .

One has:

Proposition 3.1 *Let (A, S) be an Artin-Tits system where A is of spherical type; Then, A admits the following presentation:*

$$\langle M_S \mid xf(y, x) = yf(x, y) \text{ for all } x, y \in M_S \rangle$$

and A^+ admits the same presentation as a monoid.

In the following, we fix (A_S, S) an Artin-Tits system where A_S is of spherical type. If X is a finite set, we denote by $F^*(X)$ the free monoid with base X . For w in $F^*(M_S)$ or in $F^*(M_S \cup M_S^{-1})$ we write \overline{w} to denote it's corresponding element in A . The elements of these monoids are called words; we denote by ϵ the empty word. If β is in A and w is in $F^*(M_S \cup M_S^{-1})$, we say that w represents β when $\beta = \overline{w}$. The complexity of our algorithm is calculated regarding the length ℓ on $F^*(M_S \cup M_S^{-1})$. In particular, we assume that the f -reversing function is known. Note that S is a subset of M_S .

Definition 3.2 Let $w = x_1^{\epsilon_1} \cdots x_\ell^{\epsilon_\ell}$ be in $F^*(M_S \cup M_S^{-1})$ such that the x_i are in M_S and ϵ_i are in $\{-1, 1\}$. Let $w' = ab^{-1}$ be in $F^*(M_S \cup M_S^{-1})$ with a and b in $F^*(M_S)$; hence w' does not contain any pair $x^{-1}y$ with x, y in M_S . We say that w is f -reversible into w' if there exists a finite sequence of $w = w_0, w_1, \dots, w_n = w'$ such that in step i some subword $x^{-1}y$ with x, y in M_S of w_{i-1} is replaced by $f(y, x)f(x, y)^{-1}$ in order to get w_i .

Remark 3.3 The process of f -reversing (on the right) can be duplicated into g -reversing on the left using a left complement function. In this case, during step i a subword xy^{-1} with x, y in M_S of w_{i-1} is replaced by $g(y, x)^{-1}g(x, y)$ in order to get w_i , hence in w' there will be no pairs xy^{-1} with x, y in M_S . Note that for an Artin group of spherical type, it is the same to know the f -reversing function and the g -reversing function using the symmetry of the relations.

It is well known that every word w , that represents β in A , is f -reversible on the right and g -reversible on the left. Therefore, given β in A and z that represents β , one can use the g -reversing process on z in order to write $w = w_1^{-1}w_2$ with w_1, w_2 in $F^*(M_S)$ which represents β , and then activate the f -reversing process on w resulting with ab^{-1} . By [4] Proposition 2.12 $\bar{a}\bar{b}^{-1}$ is the orthogonal splitting of β .

So our algorithm to identify and compute the root of a generator in an Artin group of spherical type is as follows:

Algorithm 3.4 (Identify generator conjugation)

Input: An element β of A represented by $w_0 = s_1^{\epsilon_1} \cdots s_\ell^{\epsilon_\ell} \in A$ where the s_i are in S and the ϵ_i are in $\{-1, 1\}$.

Output: True, if $\beta = bs^jb^{-1}$ (for some element b in A and some j), b , s and j ; False otherwise.

1. Write $w = ab^{-1}$ using the process described above such that $\bar{a}\bar{b}^{-1}$ is the orthogonal splitting of β .
2. Repeat step (2) on $b^{-1}a$, getting its orthogonal splitting $a_1b_1^{-1}$
3. If $b_1 = \epsilon$ and $a_1 = s^j$ for some s in S and j in \mathbb{N} . Return True, j, b and s ;
If $a_1 = \epsilon$ and $b_1 = s^j$ for some s in S and j in \mathbb{N} . Return True, $-j, a$ and s ;
Else return False.

3.2 Complexity

Proposition 3.5 The process of finding the orthogonal splitting of β in A represents by the word $w = x_1^{\epsilon_1} \cdots x_\ell^{\epsilon_\ell}$ with x_i in M_S is bounded by $N\ell^2/2$ steps, where N is an upper bound to the number of steps needed to compute the completion function $f(x, y)$. Moreover, the length (on M_S) of the word which represents β is not greater than ℓ .

PROOF: Since the relations in an Artin group are symmetrical the upper bound is the same for both $f(x, y)$ and $g(x, y)$. Now, the First step in the process of computing the orthogonal splitting of β , is to write β as $w_1^{-1}w_2$ using the g -reversing process on the left. For Second step one activates the f -reversing process on the result of First step. Because

in each step of the f -reversing process (and the g -reversing process) a subword $x^{-1}y$ (*resp.* xy^{-1}), where x and y are in M_S , is replaced by a word of length at most 2, the length of the word may decrease or stay the same, this shows that the length of the result is not greater than ℓ . Moreover, since in Lemma 3.9 (ii) of [5], Dehornoy proved that the number of steps needed to f -reverse a word of the form $u^{-1}v$ with $u, v \in M_S$ is bounded by $\frac{1}{4}N\ell^2$ steps, where N is the upper bound to the number of steps needed to compute the $f(x, y)$, we end with a total upper bound for the number of steps which is $2N\ell^2/4 = N\ell^2/2$. \square

Theorem 3.6 *Activating Algorithm 3.4 takes at most $O(N\ell^2)$.*

PROOF: This is an immediate consequence of Proposition 3.5 when noticing that the length of the word before doing step (2) of the Algorithm 3.4 may not increase. \square

4 Application

We finish the paper with an application for the above algorithm. Recall that braid monodromy is a homomorphism between the fundamental group of a punctured disk into the braid group, which is determined by a branch curve of a generic projection to \mathbb{C}^2 of a hyper-surface in \mathbb{CP}^n . It was suggested in [12] and in [13] to use the braid monodromy as a tool to compute the fundamental group of the complement of this branch curve, and thus to induce an invariant for the surfaces up to diffeomorphism.

The *braid monodromy factorization* was introduced in [11]. It is a product form of the image of the braid monodromy homomorphism on an ordered generating set for fundamental group of the punctured disk. In [11] it is shown that the braid monodromy factorization of the branch curve can serve under certain conditions and a specific equivalence relation, as a tool to classify surfaces up to diffeomorphism. Moreover, in [11] [Proposition 3.3] it was proved that if the branch curve is cuspidal, then all factors of the braid monodromy factorization must be half-twists to some power. Since the set of all half-twists in the braid group is the conjugacy class of its generators one can apply the algorithm presented here to each of the factors in the factorization, and test its results. If the result of Algorithm 3.4 for at least one of the factors is *False*, then the factorization cannot be a braid monodromy factorization of a cuspidal branch curve.

This can be done in $O(N\ell^2 \cdot r)$ where r is the number of elements of the factorization, ℓ is the length of the longest of all factors and N is as above.

Since in the braid group M_S is actually the set of all positive braids in which no two strings cross more than once (*permutation braids*), the number of steps needed to compute $f(x, y)$ or $g(x, y)$ is bounded by $O(n \cdot \log n)$ where n is the braid's number of strings [7]. Therefore, in this case we have a total of $O(n \cdot \log n \cdot \ell^2 \cdot r)$ operations needed to test the validity of a factorization by this method. Finally, using the standard embeddings of the Coxeter groups of type $B(n)$ and $D(n)$ in the braid group on $2n + 1$ strings (see [8] for instance), one can replace in Theorem 3.3 the constant N by $(2n + 1)\log(2n + 1)$ in these cases.

References

- [1] Brieskorn, E., and Saito, K. *Artin Gruppen und Coxeter Gruppen*, Invent. Math. **17** (1972), 245–271.
- [2] Charney, R. *Geodesic automation and growth function for Artin groups of finite type*, Math. Ann. **301** (1995), 307–324.
- [3] Dehornoy, P. *Groupes de Garside* Ann. Sc. Ec. Norm. Sup., 35 (2002) 267–306 ;
- [4] Dehornoy, P. *Groups with a complemented presentation* J. Pure Appl. Algebra **116** (1997) 115–137.
- [5] Dehornoy, P. and Paris, L. *Gaussian groups and Garside groups, two generalisations of Artin groups* Proc. London. Math. Soc (3) **79** (1999) 569–604.
- [6] Deligne, P. *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972), 273–302.
- [7] Epstein, D. B. A., Cannon, J. W., Holt, D. F., Levy, S. V. F., Paterson M. S. and Thurston, W. P., *Word Processing in Groups*, Jones and Bartlett Publishers, Boston, MA, 1992.
- [8] Eriksson H., and Eriksson K., *Affine Weyl groups as infinite permutations*, J. Comb. **5** (1998) 231–262.
- [9] Franco, N. and Gonzalez-Meneses, J., *Conjugacy problem for braid groups and Garside groups*, To appear in J. Algebra.
- [10] Godelle, E. and Paris L., *On singular Artin monoids*, Arxiv math.GR/0311346.
- [11] Kulikov, V.S. and Teicher, M., *Braid monodromy factorization and diffeomorphism types*, *Izvestiya: Mathematics* **64:2** (2000), 89–120.
- [12] Moishezon, B. and Teicher, M., *Braid group techniques in complex geometry I, Line arrangements in \mathbb{CP}^2* , Contemporary Math. **78** (1988), 425–555.
- [13] Moishezon B. and Teicher, M., *Braid Group Techniques in Complex Geometry II: From arrangements of lines to cuspidal curves*, *LNMA* **1479** (1989), 131–179.
- [14] Paris, L. *Artin monoids inject in their groups*, Comment. Math. Helv., **77** (2002), 609–637.

Godelle Eddy
Laboratoire de Mathématique Nicolas Oresme,
Université de Caen,
14032 Caen cedex, France
email: Eddy.Godelle@math.unicaen.fr

Kaplan Shmuel
Department of Mathematics and Statistics,
Bar-Ilan University,

Ramat-Gan 52900, Israel
email: kaplansh@macs.biu.ac.il

Teicher Mina
Department of Mathematics and Statistics,
Bar-Ilan University,
Ramat-Gan 52900, Israel
email: teicher@macs.biu.ac.il